

**Notice of Allowability**

Application No.

09/458,921

Examiner

Aravind K. Moorthy

Applicant(s)

PEYRAVIAN ET AL.

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to 8/2/07.
2. ☒ The allowed claim(s) is/are 1-28 and 47-50.
3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
  - a) ☐ All b) ☐ Some\* c) ☐ None of the:
    1. ☐ Certified copies of the priority documents have been received.
    2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
    3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

\* Certified copies not received: \_\_\_\_\_.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.

**THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.**

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
  - (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
    - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date \_\_\_\_\_.
  - (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date \_\_\_\_\_.Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

**Attachment(s)**

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08),  
Paper No./Mail Date \_\_\_\_\_
4. ☐ Examiner's Comment Regarding Requirement for Deposit  
of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☒ Interview Summary (PTO-413),  
Paper No./Mail Date 8/15/07
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other \_\_\_\_\_

  
CHRISTOPHER REVAK  
PRIMARY EXAMINER

### DETAILED ACTION

1. This is in response to the amendment filed on 2 August 2007.
2. Claims 1-28 and 47-50 are pending in the application.
3. Claims 1-28 and 47-50 have been allowed.
4. Claims 29-46, 51 and 52 have been allowed.

### EXAMINER'S AMENDMENT

5. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Stephen A. Herrera on 14 August 2007.

The application has been amended as follows:

Claim 15. (Currently Amended) A method for time stamping a document comprising:

receiving a time stamp request at an outside agency at a first time, said  
time stamp request comprising identifying data associated with said document;

creating at said outside agency a time stamp receipt based on said  
identifying data and a time indication;

generating at said outside agency a message authentication code based on  
said time stamp receipt and a first secret key;

encrypting the first secret key with a second secret key to generate a an  
encrypted key message;

generating a second message authentication code based on said first message authentication code and said first secret key using a third secret key;

transmitting said time stamp receipt, said first message authentication code, said second message authentication code, and said key message to said requestor;

receiving at said outside agency at a second time a certification request, said certification request comprising said time stamp receipt, said first message authentication code, said second message authentication code, and said encrypted key message;

decrypting at said outside agency said encrypted key message to recover said first secret key;

validating said second message authentication code at said outside agency using said third secret key;

validating said first message authentication code at said outside agency using said first secret key if said second message authentication code is valid; and

certifying said time stamp receipt at said outside agency using a cryptographic signature scheme if said first message authentication code is valid.

*Allowable Subject Matter*

6. Claims 1-28 and 47-50 are allowed.

The following is an examiner's statement of reasons for allowance:

The current application is directed towards a time stamping protocol that has two stages referred to as the ticketing stage and the certification stage. During the ticketing stage, the document or other identifying data is sent to the TSA. The TSA generates a "ticket" based on the document or other identifying data and a time indication derived from a trusted clock. The ticket, which serves as an unsigned time stamp receipt, is transmitted back to the document originator. During the certification stage, the holder of the ticket requests a certified time stamp receipt by presenting the ticket to the TSA. The TSA verifies the ticket and generates a signed time stamp receipt, called the ticket stub, which is then transmitted back to the document originator. The ticket stub serves as a "universal time-stamp" that the holder of the ticket stub can use to prove the date of the document.

The closest prior art to the current application was Haber et al U.S. Patent No. 5,781,629 (hereinafter Haber). Haber is directed towards a process for time-stamping a digital document. The process provides a certificate which not only allows for the authentication of a document at a later time but which includes a name or nickname which allows for the unique identification of the document at a later time. The name or nickname provided in accordance with the present invention is not only simple and concise but allows for the self-authentication of the document that it refers to. The name can be used when two independent parties desire to refer to the same unique document in a quick and simple way.

However, Haber differs from the current application in several aspects. Haber fails to teach a message authentication code. Haber does not teach or suggest the two-stage certification process set forth in the claims. Haber discloses a conventional time stamping process wherein the time stamping authority appends a time stamp to identifying data received from the requestor and immediately certifies the time stamp receipt by signing the time stamp receipt with a private signature key. Claims 1 and 15 both require that a time stamp request and a certification request be presented to the time stamping authority at two distinct times. Claims 1 and 15 require generating a message authentication code at a first time and certifying the time stamp receipt at a second time only if the message authentication code is valid. Haber does not teach or suggest this claimed two-step process.

Any claims not directly addressed are allowed the virtue of their dependency.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."


Art Unit: 2131

*Conclusion*

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K. Moorthy whose telephone number is 571-272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Aravind K Moorthy   
August 15, 2007

CHRISTOPHER REVAK  
PRIMARY EXAMINER

